

Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking **High**. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - Web Vulnerability Scanner Denial of Service
  - BrightStor ARCserve Backup Arbitrary Code Execution or Denial of Service
  - Microsoft Agent Could Allow Spoofing
  - Microsoft ActiveSync Information Disclosure or Denial of Service
  - Microsoft Internet Explorer Arbitrary Code Execution
  - **Microsoft Internet Explorer Denial of Service (Updated)**
  - Microsoft Internet Explorer Web Folder Behaviors Information Disclosure or Arbitrary Code Execution
  - Microsoft Plug and Play Arbitrary Code Execution or Elevated Privileges
  - Microsoft Remote Desktop Protocol Denial of Service
  - Microsoft Telephony Service Remote Code Execution
  - Microsoft Windows Kerberos PKINIT Information Disclosure or Denial of Service
  - Microsoft Windows Print Spooler Arbitrary Code Execution
  - **Microsoft Word Remote Code Execution and Escalation of Privilege Vulnerabilities (Updated)**
  - Naxtor e-Directory Cross-Site Scripting or SQL Injection
  - Naxtor Shopping Cart Cross-Site Scripting or SQL Injection
  - NetworkActiv Web Server Cross-Site Scripting
  - Quick 'n Easy FTP Server Denial of Service
  - ProRat Server Arbitrary Code Execution
  - Symantec Norton GoBack Lets Local Users Bypass Authentication
- UNIX / Linux Operating Systems
  - **Clam AntiVirus Multiple Vulnerabilities (Updated)**
  - Debian Apt-Cacher Remote Arbitrary Code Execution
  - **Gzip Zgrep Arbitrary Command Execution (Updated)**
  - **Heartbeat Arbitrary File Overwrite (Updated)**
  - **Kadu Denial of Service (Updated)**
  - Lantronix Secure Console Server SCS820/SCS1620 Multiple Local Vulnerabilities
  - **Multiple Vendors Kerberos V5 Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel 64 Bit 'AR-RSC' Register Access (Updated)**
  - **Multiple Vendors Linux Kernel Race Condition and Buffer Overflow (Updated)**
  - Multiple Vendors Linux Kernel Stack Fault Exceptions Denial of Service
  - **Multiple Vendors Linux Kernel Futex Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Netfilter Memory Leak Denial of Service (Updated)**
  - **Multiple Vendor Linux Kernel pktcdvd & raw device Block Device (Updated)**
  - **Multiple Vendors Linux Kernel SYSFS Write File Local Integer Overflow (Updated)**
  - Multiple Vendors Linux Kernel NFSACL Protocol XDR Data Remote Denial of Service
  - **Multiple Vendors Linux Kernel Auditing Code Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Vulnerabilities (Updated)**
  - Multiple Vendors Linux Kernel XFRM Array Index Buffer Overflow
  - Multiple Vendors Linux Kernel Management Denials of Service
  - **Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service (Updated)**
  - **netpbm Arbitrary Code Execution (Updated)**
  - **ProFTPD Denial of Service or Information Disclosure (Updated)**
  - Sun Solaris Printd Arbitrary File Deletion
  - SysCP Multiple Script Execution
  - Wine Wine Launcher.IN Local Insecure File Creation
  - **Wojtek Kaniewski EKG Insecure Temporary File Creation (Updated)**
  - **Wojtek Kaniewski EKG Insecure Temporary File Creation & SQL Injection (Updated)**
  - **Yukihiko Matsumoto Ruby XMLRPC Server Unspecified Command Execution (Updated)**
- Multiple Operating Systems
  - Apache HTTP Request Smuggling Vulnerability
  - Chipmunk Forum 'fontcolor' Cross-Site Scripting
  - **Cisco IOS Remote Denial of Service or Arbitrary Code Execution (Updated)**
  - Comdev eCommerce 'WCE.Download.PHP' Directory Traversal

- [Comdev ECommerce Config.PHP Remote File Include](#)
- [Denora IRC Stats Remote Buffer Overflow](#)
- [E107 Website System Cross-Site Scripting & HTML Injection](#)
- [EMC Navisphere Manager IEMC Navisphere Manager Directory Traversal & Information Disclosure](#)
- [Ethereal Denial of Service or Arbitrary Code Execution \(Updated\)](#)
- [FFTW Insecure Temporary File Creation](#)
- [FlatNuke Multiple Vulnerabilities](#)
- [FunkBoard Multiple Cross-Site Scripting](#)
- [Fusebox 'Index.CFM' Cross-Site Scripting](#)
- [Gravity Board X Input Validation & Access Restrictions](#)
- [Inkscape 'ps2epsi.sh' Insecure Temporary File](#)
- [Invision Power Board Cross-Site Scripting](#)
- [Jax PHP Scripts Multiple Cross-Site Scripting](#)
- [Jax PHP Scripts Multiple Remote Information Disclosure](#)
- [Karrigell Arbitrary Python Code Execution](#)
- [KDE Kate, KWrite Local Backup File Information Disclosure \(Updated\)](#)
- [Lansoft Enterprises OpenBB Multiple SQL Injection](#)
- [LogiCampus Helpdesk Cross-Site Scripting](#)
- [McDATA E/OS Remote Denial of Service](#)
- [Metasploit Framework MSFWeb Defanged Mode Restriction Bypass](#)
- [MyFAQ Multiple SQL Injection](#)
- [MySQL User-Defined Function Buffer Overflow](#)
- [PHP-Fusion 'Messages.PHP' SQL Injection](#)
- [PHPLite Calendar Express SQL Injection & Cross-Site Scripting](#)
- [PHPMailer 'Data\(\)' Function Remote Denial of Service \(Updated\)](#)
- [PHPOpenChat Multiple Cross-Site Scripting](#)
- [PHPSiteStats Authentication Bypass](#)
- [PortailPHP 'Index.PHP' SQL Injection](#)
- [Silvernews 'Admin.PHP' SQL Injection](#)
- [SquirrelMail Cross-Site Scripting Vulnerabilities \(Updated\)](#)
- [SquirrelMail Variable Handling \(Updated\)](#)
- [TDiary Cross-Site Request Forgery](#)
- [Web Content Management Cross-Site Scripting & Authentication Bypass](#)
- [XMB Forum U2U.Inc.PHP SQL Injection](#)

[Wireless](#)

[Recent Exploit Scripts/Techniques](#)

[Trends](#)

[Viruses/Trojans](#)

## Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the [Multiple Operating Systems](#) section.

*Note: All the information included in the following tables has been discussed in newsgroups and on web sites.*

### The Risk levels defined below are based on how the system may be impacted:

*Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.*

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Acunetix Web Vulnerability Scanner 2.0	<p>A vulnerability has been reported in Web Vulnerability Scanner (Web Sniffer) that could let remote malicious users cause a Denial of Service.</p> <p>No workaround or patch available at time of publishing.</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Web Vulnerability Scanner Denial of Service	Low	Security Tracker, Alert ID: 1014628, August 5, 2005

Computer Associates	Multiple buffer overflow vulnerabilities have been reported in BrightStor ARCserve Backup that could let remote malicious users execute arbitrary code.  A vendor patch is available: <a href="http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=33239">http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=33239</a>  An exploit has been published.	BrightStor ARCserve Backup Arbitrary Code  <a href="#">CAN-2005-1272</a> <a href="#">CAN-2005-0260</a>	High	Computer Associates, Vulnerability ID: 33239, August 2, 2005  US-CERT, <a href="#">VU#279774</a> , <a href="#">VU#966880</a> , <a href="#">VU#864801</a>
Microsoft  Windows 2000, XP, Server 2003, 98, 98 (SE), (ME)	A spoofing vulnerability has been reported that could enable a malicious user to spoof trusted Internet content.  Updates available: <a href="http://www.microsoft.com/technet/security/Bulletin/MS05-032.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-032.msp</a>  <b>V2.0: Update available for x64-based systems, Microsoft Windows Server 2003 for Itanium-based Systems, and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems.</b>  Currently we are not aware of any exploits for this vulnerability.	Microsoft Agent Could Allow Spoofing  <a href="#">CAN-2005-1214</a>	Medium	Microsoft, MS05-032, June 14, 2004  <a href="#">US-CERT VU#718542</a>  <b>Microsoft Security Bulletin MS05-032, August 9, 2005</b>
Microsoft  ActiveSync 3.8, 3.7.1	Multiple vulnerabilities have been reported in ActiveSync's network synchronization protocol that could let remote malicious users to disclose information or cause a Denial of Service.  No workaround or patch available at time of publishing.  There is no exploit code required.	Microsoft ActiveSync Information Disclosure or Denial of Service	Medium	Security Focus, 14457, August 2, 2005
Microsoft  Internet Explorer	A memory corruption vulnerability has been reported in Internet Explorer COM Object instantiation that could let remote malicious users execute arbitrary code.  Vendor fix available: <a href="http://www.microsoft.com/technet/security/Bulletin/MS05-038.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-038.msp</a>  A Proof of Concept exploit has been published.	Microsoft Internet Explorer Arbitrary Code Execution  <a href="#">CAN-2005-1990</a>	High	Microsoft Security Bulletin MS05-038, August 9, 2005  <a href="#">US-CERT VU#959049</a>
Microsoft  Internet Explorer 6.0SP2	Multiple vulnerabilities have been reported in Internet Explorer, JPEG Rendering, that could let remote malicious users perform a Denial of Service.  <b>Vendor fix available:</b> <a href="http://www.microsoft.com/technet/security/Bulletin/MS05-038.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-038.msp</a>  A Proof of Concept exploit has been published.	Microsoft Internet Explorer Denial of Service  <a href="#">CAN-2005-2308</a> <a href="#">CAN-2005-1988</a>	Low	Security Focus, 14284, 14285, 14286, July 15, 2005  <b>Microsoft Security Bulletin MS05-038, August 9, 2005</b>  <a href="#">US-CERT VU#965206</a>
Microsoft  Internet Explorer Web Folder Behaviors	A vulnerability has been reported in Internet Explorer that could let remote malicious users disclose information or execute arbitrary code.  Vendor fix available: <a href="http://www.microsoft.com/technet/security/Bulletin/MS05-038.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-038.msp</a>  Currently we are not aware of any exploits for this vulnerability.	Microsoft Internet Explorer Web Folder Behaviors Information Disclosure or Arbitrary Code Execution  <a href="#">CAN-2005-1989</a>	High	Microsoft Security Bulletin MS05-038, August 9, 2005
Microsoft  Plug and Play	A vulnerability has been reported in Plug and Play that could let local or remote malicious users execute arbitrary code or obtain elevated privileges.  Vendor fix available: <a href="http://www.microsoft.com/technet/security/Bulletin/MS05-039.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-039.msp</a>  Currently we are not aware of any exploits for this vulnerability.	Microsoft Plug and Play Arbitrary Code Execution or Elevated Privileges  <a href="#">CAN-2005-1983</a>	High	Microsoft Security Bulletin MS05-039, August 9, 2005  <a href="#">US-CERT VU#998653</a>
Microsoft  Remote Desktop Protocol	A vulnerability has been reported in Remote Desktop Protocol that could let remote malicious users cause a Denial of Service.  Vendor fix available: <a href="http://www.microsoft.com/technet/security/Bulletin/MS05-041.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-041.msp</a>  A Proof of Concept exploit has been published.	Microsoft Remote Desktop Protocol Denial of Service  <a href="#">CAN-2005-1218</a>	Low	Microsoft Security Bulletin MS05-041, August 9, 2005  <a href="#">US-CERT VU#490628</a>
Microsoft  Telephony Service	A buffer overflow vulnerability has been reported in Microsoft Telephony Service that could let local or remote malicious users execute arbitrary code.  Vendor fix available: <a href="http://www.microsoft.com/technet/security/Bulletin/MS05-040.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-040.msp</a>  Currently we are not aware of any exploits for this vulnerability.	Microsoft Telephony Service Remote Code Execution  <a href="#">CAN-2005-0058</a>	High	Microsoft Security Bulletin MS05-040, August 9, 2005

Microsoft Windows Kerberos PKINT	<p>Multiple vulnerabilities have been reported in Windows Kerberos PKINT that could let remote malicious users disclose information or cause a Denial of Service.</p> <p>Vendor fix available:  <a href="http://www.microsoft.com/technet/security/Bulletin/MS05-042.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-042.msp</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Microsoft Windows Kerberos PKINIT Information Disclosure or Denial of Service	Low	Microsoft Security Bulletin MS05-042, August 9, 2005
Microsoft Windows Print Spooler in XP, 2000, Server 2003	<p>A buffer overflow vulnerability has been reported in Windows Print Spooler that could let local or remote malicious users execute arbitrary code.</p> <p>Vendor fix available:  <a href="http://www.microsoft.com/technet/security/Bulletin/MS05-043.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-043.msp</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Microsoft Windows Print Spooler Arbitrary Code Execution	High	Microsoft Security Bulletin MS05-043, August 9, 2005  <a href="#">US-CERT VU#220821</a>
Microsoft Word 2000, 2002  Works Suite 2001, 2002, 2003, and 2004  Office Word 2003  Microsoft Word 2003 Viewer	<p>A buffer overflow vulnerability has been reported that could lead to remote execution of arbitrary code or escalation of privilege.</p> <p>V1.1 Bulletin updated to point to the correct Exchange 2000 Server Post-Service Pack 3 (SP3) Update Rollup and to advise on the scope and caveats of workaround "Unregister xlsasink.dll and fallback to Active Directory for distribution of route information."</p> <p><b>V2.0 Microsoft Word 2003 Viewer also affected.</b></p> <p>Updates available:  <a href="http://www.microsoft.com/technet/security/Bulletin/MS05-023.msp">http://www.microsoft.com/technet/security/Bulletin/MS05-023.msp</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Microsoft Word Remote Code Execution and Escalation of Privilege Vulnerabilities	High	Microsoft Security Bulletin MS05-023, April 12, 2005  <a href="#">US-CERT VU#442567</a>  <a href="#">US-CERT VU#752591</a>  Microsoft Security Bulletin MS05-023 V1.1, April 14, 2005  <b>Microsoft Security Bulletin MS05-023 V1.1, August 9, 2005</b>
Naxtor Technologies Naxtor e-Directory 1.0	<p>A vulnerability has been reported in Naxtor e-Directory that could let remote malicious users to conduct Cross-Site Scripting and perform SQL injection.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	Naxtor e-Directory Cross-Site Scripting or SQL Injection	Medium	Secunia, Advisory: SA16314, August 3, 2005
Naxtor Technologies Naxtor Shopping Cart 1.0, Pro 1.0	<p>Multiple vulnerabilities has been reported in Naxtor Shopping Cart that could let remote malicious users to conduct Cross-Site Scripting or perform SQL injection.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	Naxtor Shopping Cart Cross-Site Scripting or SQL Injection	Medium	Security Focus, 14454, 14456, August 2, 2005
NetowrkActiv NetworkActiv Web Server 3.5.13 and previous	<p>An input validation vulnerability has been reported in NetworkActiv Web Server that could let remote malicious users conduct Cross-Site Scripting.</p> <p>Upgrade to V3.5.14:  <a href="http://www.networkactiv.com/WebServer.html">http://www.networkactiv.com/WebServer.html</a></p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	NetworkActiv Web Server Cross-Site Scripting	Medium	Secunia, Advisory: SA16301, August 4, 2005
Pablo Software Solutions Quick 'n Easy FTP Server 3.0	<p>An input validation vulnerability has been reported in Quick 'n Easy FTP Server (USER Command) that could let remote malicious users cause a Denial of Service.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	Quick 'n Easy FTP Server Denial of Service	Low	Security Tracker, Alert ID: 1014615, August 3, 2005
ProRat Server 1.9 Fix2	<p>A buffer overflow vulnerability has been reported in ProRat Server that could let remote malicious users execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	ProRat Server Arbitrary Code Execution	High	Security Focus, 14458, August 2, 2005
Symantec Norton GoBack 4.0	<p>A vulnerability has been reported in Norton GoBack that could let local malicious users bypass authentication.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	Norton GoBack Authentication Bypass	Medium	Security Tracker Alert ID: 1014612, August 2, 2005

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Clam AntiVirus 0.86.1	<p>Multiple vulnerabilities have been reported in Clam AntiVirus that could let remote malicious users cause a Denial of Service.</p> <p>Upgrade to version 0.86.2:  <a href="http://www.clamav.net/stable.php#pagestart">http://www.clamav.net/stable.php#pagestart</a></p> <p><b>Conectiva:</b>  <a href="ftp://atualizacoes.conectiva.com.br/">ftp://atualizacoes.conectiva.com.br/</a></p> <p><b>Mandriva:</b>  <a href="http://www.mandriva.com/security/advisories?name=MDKSA-2005:125">http://www.mandriva.com/security/advisories?name=MDKSA-2005:125</a></p> <p><b>Gentoo:</b>  <a href="http://security.gentoo.org/glsa/glsa-200507-25.xml">http://security.gentoo.org/glsa/glsa-200507-25.xml</a></p> <p><b>SUSE:</b>  <a href="ftp://ftp.SUSE.com/pub/SUSE">ftp://ftp.SUSE.com/pub/SUSE</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Clam AntiVirus Multiple Vulnerabilities</p> <p><a href="#">CAN-2005-2450</a></p>	Low	<p>Secunia, Advisory: SA16180, July 25, 2005</p> <p><b>Gentoo Linux Security Advisory GLSA 200507-25</b>, July 26, 2005</p> <p><b>Mandriva Security Advisory, MDKSA-2005:125</b>, July 27, 2005</p> <p><b>SUSE Security Summary Report, SUSE-SR:2005:018</b>, July 28, 2005</p> <p><b>Conectiva Linux Announcement, CLSA-2005:987</b>, July 29, 2005</p>
Debian  apt-cacher 0.9.9, 0.9.4	<p>A vulnerability has been reported due to an unspecified input validation error, which could let a remote malicious user execute arbitrary code.</p> <p>Debian:  <a href="http://www.debian.org/security/2005/dsa-772">http://www.debian.org/security/2005/dsa-772</a></p> <p>There is no exploit code required.</p>	<p>Debian Apt-Cacher Remote Arbitrary Code Execution</p> <p><a href="#">CAN-2005-1854</a></p>	High	<p>Debian Security Advisory, DSA 772-1, August 3, 2005</p>
GNU  zgrep 1.2.4	<p>A vulnerability has been reported in 'zgrep.in' due to insufficient validation of user-supplied arguments, which could let a remote malicious user execute arbitrary commands.</p> <p>A patch for 'zgrep.in' is available in the following bug report:  <a href="http://bugs.gentoo.org/show_bug.cgi?id=90626">http://bugs.gentoo.org/show_bug.cgi?id=90626</a></p> <p><b>Mandriva:</b>  <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a></p> <p><b>TurboLinux:</b>  <a href="ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/">ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/</a></p> <p><b>RedHat:</b>  <a href="http://rhn.redhat.com/errata/RHSA-2005-357.html">http://rhn.redhat.com/errata/RHSA-2005-357.html</a></p> <p><b>RedHat:</b>  <a href="http://rhn.redhat.com/errata/RHSA-2005-474.html">http://rhn.redhat.com/errata/RHSA-2005-474.html</a></p> <p><b>SGI:</b>  <a href="ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/">ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/</a></p> <p><b>Fedora:</b>  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/</a></p> <p><b>SGI:</b>  <a href="http://www.sgi.com/support/security/">http://www.sgi.com/support/security/</a></p> <p><b>F5:</b>  <a href="http://tech.f5.com/home/bigip/solutions/advisories/sol4532.html">http://tech.f5.com/home/bigip/solutions/advisories/sol4532.html</a></p> <p><b>Ubuntu:</b>  <a href="http://security.ubuntu.com/ubuntu/pool/main/g/gzip/">http://security.ubuntu.com/ubuntu/pool/main/g/gzip/</a></p> <p><b>Trustix:</b></p>	<p>Gzip Zgrep Arbitrary Command Execution</p> <p><a href="#">CAN-2005-0758</a></p>	High	<p>Security Tracker Alert, 1013928, May 10, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005</p> <p>Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005</p> <p>RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005</p> <p>RedHat Security Advisory, RHSA-2005:474-15, June 16, 2005</p> <p>SGI Security Advisory, 20050603-01-U, June 23, 2005</p> <p>Fedora Update Notification, FEDORA-2005-471, June 27, 2005</p> <p>SGI Security Advisory, 20050605-01-U, July 12, 2005</p> <p>Secunia Advisory: SA16159, July 21, 2005</p> <p><b>Ubuntu Security Notice,</b></p>

	<a href="ftp://ftp.trustix.org/pub/trustix/updates/">ftp://ftp.trustix.org/pub/trustix/updates/</a>  There is no exploit code required.			<b>USN-158-1, August 01, 2005</b>  <b>Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005</b>
High Availability Linux Project  Heartbeat 1.2.3	An insecure file creation vulnerability has been reported in Heartbeat that could let local users arbitrarily overwrite files.  Debian: <a href="http://security.debian.org/pool/updates/main/h/heartbeat/">http://security.debian.org/pool/updates/main/h/heartbeat/</a>  <b>Conectiva:</b> <a href="ftp://atualizacoes.conectiva.com.br">ftp://atualizacoes.conectiva.com.br</a>  <b>Gentoo:</b> <a href="http://security.gentoo.org/glsa/glsa-200508-05.xml">http://security.gentoo.org/glsa/glsa-200508-05.xml</a>  There is no exploit code required.	Heartbeat Arbitrary File Overwrite  <a href="#">CAN-2005-2231</a>	Medium	Secunia Advisory: SA16039, July 12, 2005  Debian Security Advisory, DSA 761-1, July 19, 2005  <b>Conectiva Linux Announcement, CLSA-2005:991, August 4, 2005</b>  <b>Gentoo Linux Security Advisory, GLSA 200508-05, August 7, 2005</b>
Kadu  Kadu 0.4.0	An integer overflow vulnerability has been reported in Kadu (libgadu) which could let remote malicious users cause a Denial of Service.  Upgrade to version 0.4.1: <a href="http://www.kadu.net/wiki/index.php/English:Main_Page">http://www.kadu.net/wiki/index.php/English:Main_Page</a>  Gentoo: <a href="http://www.gentoo.org/security/en/glsa/glsa-200507-26.xml">http://www.gentoo.org/security/en/glsa/glsa-200507-26.xml</a>  <b>Conectiva:</b> <a href="ftp://atualizacoes.conectiva.com.br/">ftp://atualizacoes.conectiva.com.br/</a>  <b>Ubuntu:</b> <a href="http://security.ubuntu.com/ubuntu/pool/main/e/ekg/">http://security.ubuntu.com/ubuntu/pool/main/e/ekg/</a>  Currently we are not aware of any exploits for this vulnerability.	Kadu Denial of Service  <a href="#">CAN-2005-1852</a>	Low	Secunia, Advisory: SA16238, July 27, 2005  Gentoo Security Advisory, GLSA 200507-26, July 27, 2005  <b>Conectiva Linux Announcement, CLSA-2005:989, August 4, 2005</b>  <b>Ubuntu Security Notice, USN-162-1, August 08, 2005</b>
Lantronix  Lantronix SCS82, SCS1620	Multiple vulnerabilities have been reported: a vulnerability was reported due in '/tmp' due to insecure pipe permissions, which could let a malicious user read arbitrary files with elevated privileges; a Directory Traversal vulnerability was reported in the console command interface, which could let a malicious user obtain sensitive information; a vulnerability was reported in the command-line interface, which could let a malicious user obtain superuser privileges; and a buffer overflow vulnerability was reported in the 'edituser' binary due to a boundary error, which could let a malicious user execute arbitrary code with root privileges.  Updated firmware available at: <a href="ftp://ftp.lantronix.com/pub/scs1620/">ftp://ftp.lantronix.com/pub/scs1620/</a>  A Proof of Concept exploit has been published for the 'edituser' buffer overflow vulnerability.	Lantronix Secure Console Server SCS820/SCS1620 Multiple Local Vulnerabilities	High	Security Focus, 14486, August 5, 2005

Multiple Vendors Turbolinux Server 10.0, 8.0, Desktop 10.0, Turbolinux Home Appliance Server 1.0 Workgroup Edition, Hosting Edition; Trustix Secure Linux 3.0, 2.2, Secure Enterprise Linux 2.0; Sun Solaris 10.0 _x86, 10.0, 9.0 _x86 Update 2, 9.0 _x86, 9.0, Sun SEAM 1.0-1.0.2; SuSE Linux Professional 9.3 x86_64, 9.3, Linux Personal 9.3 x86_64, 9.3; RedHat Fedora Core3 & 4, Advanced Workstation for the Itanium Processor 2.1; MIT Kerberos 5 5.0 -1.4.1 & prior; Gentoo Linux	<p>Multiple vulnerabilities have been reported: a remote Denial of Service vulnerability was reported when a malicious user submits a specially crafted TCP connection that causes the Key Distribution Center (KDC) to attempt to free random memory; a buffer overflow vulnerability was reported in KDC due to a boundary error when a specially crafted TCP or UDP request is submitted, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported in 'krb/recvauth.c' which could let a remote malicious user execute arbitrary code.</p> <p>MIT: <a href="http://web.mit.edu/kerberos/advisories/2005-002-patch_1.4.1.txt.asc">http://web.mit.edu/kerberos/advisories/2005-002-patch_1.4.1.txt.asc</a></p> <p>Mandriva: <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a></p> <p>Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates">http://download.fedora.redhat.com/pub/fedora/linux/core/updates</a></p> <p>RedHat: <a href="http://rhn.redhat.com/errata/RHSA-2005-567.html">http://rhn.redhat.com/errata/RHSA-2005-567.html</a></p> <p>Sun: <a href="http://sunsolve.sun.com/search/document.do?assetkey=1-26-101809-1">http://sunsolve.sun.com/search/document.do?assetkey=1-26-101809-1</a></p> <p>SuSE: <a href="http://www.novell.com/linux/security/advisories.html">http://www.novell.com/linux/security/advisories.html</a></p> <p>Trustix: <a href="http://http.trustix.org/pub/trustix/updates/">http://http.trustix.org/pub/trustix/updates/</a></p> <p>TurboLinux: <a href="ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/">ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/</a></p> <p>SGI: <a href="http://www.sgi.com/support/security/">http://www.sgi.com/support/security/</a></p> <p>Debian: <a href="http://www.debian.org/security/2005/dsa-757">http://www.debian.org/security/2005/dsa-757</a></p> <p><b>Conectiva:</b> <a href="http://distro.conectiva.com.br/atualizacoes/index.php?id=a&amp;anuncio=000993">http://distro.conectiva.com.br/atualizacoes/index.php?id=a&amp;anuncio=000993</a></p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	Kerberos V5 Multiple Vulnerabilities  <a href="#">CAN-2005-1174</a> <a href="#">CAN-2005-1175</a> <a href="#">CAN-2005-1689</a>	High	<p>MIT krb5 Security Advisory, 2005-002, July 12, 2005</p> <p>RedHat Security Advisory, RHSA-2005:567-08, July 12, 2005</p> <p>Sun(sm) Alert Notification, 101809, July 12, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-552 &amp; 553, July 12, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005</p> <p>Turbolinux Security Advisory TLSA-2005-78, July 13, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:119, July 14, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0036, July 14, 2005</p> <p>SGI Security Advisory, 20050703-01-U, July 15, 2005</p> <p>Debian Security Advisory, DSA-757-1, July 17, 2005</p> <p><a href="#">US-CERT VU#885830</a></p> <p><a href="#">US-CERT VU#623332</a></p> <p><a href="#">US-CERT VU#259798</a></p> <p><b>Conectiva Linux Advisory, CLSA-2005:993, August 8, 2005</b></p>
Multiple Vendors  Linux kernel 2.6 prior to 2.6.12.1	<p>A vulnerability has been reported in the 'restore_sigcontext()' function due to a failure to restrict access to the 'ar.rsc' register, which could let a malicious user cause a Denial of Service or obtain elevated privileges.</p> <p>Updates available at: <a href="http://www.kernel.org/">http://www.kernel.org/</a></p> <p><b>SUSE:</b> <a href="http://www.novell.com/linux/security/advisories/2005_44_kernel.html">http://www.novell.com/linux/security/advisories/2005_44_kernel.html</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Linux Kernel 64 Bit 'AR-RSC' Register Access  <a href="#">CAN-2005-1761</a>	Medium	<p>Security Tracker Alert ID: 1014275, June 23, 2005</p> <p><b>SUSE Security Announcement, SUSE-SA:2005:044, August 4, 2005</b></p>

Multiple Vendors  Linux Kernel 2.4, 2.6	<p>A race condition in ia32 emulation, vulnerability has been reported in the Linux Kernel that could let local malicious users obtain root privileges or create a buffer overflow.</p> <p>Patch Available:  <a href="http://kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32-pre1.bz2">http://kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.32-pre1.bz2</a></p> <p>Trustix:  <a href="http://http.trustix.org/pub/trustix/updates/">http://http.trustix.org/pub/trustix/updates/</a></p> <p><b>SUSE:</b>  <a href="ftp://ftp.SUSE.com/pub/SUSE">ftp://ftp.SUSE.com/pub/SUSE</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Linux Kernel Race Condition and Buffer Overflow  <a href="#">CAN-2005-1768</a>	High	<p>Security Focus, 14205, July 11, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0036, July 14, 2005</p> <p><b>SUSE Security Announcement, SUSE-SA:2005:044, August 4, 2005</b></p>
Multiple Vendors  SuSE Linux Professional 9.0, x86_64; Linux kernel 2.6-2.6.12, 2.5 .0- 2.5.69, 2.4-2.4.32	<p>An unspecified Denial of Service vulnerability has been reported when stack fault exceptions are triggered.</p> <p>SUSE:  <a href="ftp://ftp.SUSE.com/pub/SUSE">ftp://ftp.SUSE.com/pub/SUSE</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Linux Kernel Stack Fault Exceptions Denial of Service  <a href="#">CAN-2005-1767</a>	Low	<p>Security Focus, 14467, August 3, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:044, August 4, 2005</p>
Multiple Vendors  Linux kernel 2.5.0-2.5.69, 2.6-2.6.11	<p>A Denial of Service vulnerability has been reported in 'kernel/futex.c.'</p> <p>Ubuntu:  <a href="http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/">http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/</a></p> <p><b>RedHat:</b>  <a href="http://rhn.redhat.com/errata/RHSA-2005-420.html">http://rhn.redhat.com/errata/RHSA-2005-420.html</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Linux Kernel Futex Denial of Service  <a href="#">CAN-2005-0937</a>	Low	<p>Security Tracker Alert, 1013616, March 31, 2005</p> <p>Ubuntu Security Notice, USN-110-1 April 11, 2005</p> <p><b>RedHat Security Advisory, RHSA-2005:420-24, Updated August 9, 2005</b></p>
Multiple Vendors  Linux kernel 2.6 .10, Linux kernel 2.6 -test1-test11, 2.6-2.6.8	<p>A Denial of Service vulnerability has been reported in the Netfilter code due to a memory leak.</p> <p>Ubuntu:  <a href="http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/">http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/</a></p> <p>SuSE:  <a href="ftp://ftp.suse.com/pub/suse/">ftp://ftp.suse.com/pub/suse/</a></p> <p>Fedora:  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p>Conectiva:  <a href="ftp://atualizacoes.conectiva.com.br/10/">ftp://atualizacoes.conectiva.com.br/10/</a></p> <p>Fedora:  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p><b>RedHat:</b>  <a href="http://rhn.redhat.com/errata/RHSA-2005-366.html">http://rhn.redhat.com/errata/RHSA-2005-366.html</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Linux Kernel Netfilter Memory Leak Denial of Service  <a href="#">CAN-2005-0210</a>	Low	<p>Ubuntu Security Notice, USN-95-1 March 15, 2005</p> <p>SUSE Security Announcement, SUSE-SA: 2005: 018, March 24, 2005</p> <p>Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005</p> <p>Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005</p> <p>Fedora Update Notification FEDORA-2005-313, April 11, 2005</p> <p><b>RedHat Security Advisory, RHSA-2005:366-21, August 9, 2005</b></p>
Multiple Vendors  Linux Kernel 2.6 up to & including 2.6.12-rc4	<p>Several vulnerabilities have been reported: a vulnerability was reported in raw character devices (raw.c) because the wrong function is called before passing an ioctl to the block device, which crosses security boundaries by making kernel address space accessible from user space; and a vulnerability was reported in the 'pkt_ioctl' function in the 'pktcdvd' block device ioctl handler (pktcdvd.c) because the wrong function is called before passing an ioctl to the block device, which could let a malicious user execute arbitrary code.</p> <p>Update available at:</p>	Multiple Vendor Linux Kernel pktcdvd & raw device Block Device  <a href="#">CAN-2005-1264</a> <a href="#">CAN-2005-1589</a>	High	<p>Secunia Advisory, SA15392, May 17, 2005</p> <p>Ubuntu Security Notice, USN-131-1, May 23, 2005</p> <p><b>RedHat Security Advisory, RHSA-2005:420-24,</b></p>

	<a href="http://kernel.org/">http://kernel.org/</a>  Ubuntu: <a href="http://security.ubuntu.com/ubuntu/pool/main//">http://security.ubuntu.com/ubuntu/pool/main//</a>  <b>RedHat:</b> <a href="http://rhn.redhat.com/errata/RHSA-2005-420.html">http://rhn.redhat.com/errata/RHSA-2005-420.html</a>  A Proof of Concept Denial of Service exploit script has been published.			<b>Updated</b> <b>August 9, 2005</b>
Multiple Vendors  Linux kernel 2.6-2.6.11	A vulnerability has been reported in the '/sys' file system due to a mismanagement of integer signedness, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.  <b>SuSE:</b> <a href="ftp://ftp.suse.com/pub/suse/">ftp://ftp.suse.com/pub/suse/</a>  Ubuntu: <a href="http://security.ubuntu.com/ubuntu/pool/main//linux-source-2.6.8.1/">http://security.ubuntu.com/ubuntu/pool/main//linux-source-2.6.8.1/</a>  RedHat: <a href="http://rhn.redhat.com/errata/RHSA-2005-366.html">http://rhn.redhat.com/errata/RHSA-2005-366.html</a>  Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SYSFS_Write_ File Local Integer Overflow  <a href="#">CAN-2005-0867</a>	Low/ <b>High</b>  (High if arbitrary code can be executed)	Security Focus, 13091, April 11, 2005  RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005  <b>SUSE Security            Announce-            ment,            SUSE-SA:2005:044,            August 4, 2005</b>
Multiple Vendors  SuSE Linux Professional 9.3, x86_64, 9.2, x86_64, Linux Personal 9.3, x86_64; Linux kernel 2.6-2.6.12	A remote Denial of Service vulnerability has been reported in the NFSACL protocol when handling when handling XDR data.  SUSE: <a href="ftp://ftp.SUSE.com/pub/SUSE">ftp://ftp.SUSE.com/pub/SUSE</a>  Currently we are not aware of any exploits for this vulnerability.	Linux Kernel NFSACL Protocol XDR Data Remote Denial of  <a href="#">CAN-2005-2500</a>	Low	Security Focus, 14468, August 3, 2005  SUSE Security Announce- ment, SUSE-SA:2005:044, August 4, 2005
Multiple Vendors  RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; Linux kernel 2.6.9, 2.6-2.6.8	A Denial of Service vulnerability has been reported in the auditing code.  <b>RedHat:</b> <a href="http://rhn.redhat.com/errata/RHSA-2005-420.html">http://rhn.redhat.com/errata/RHSA-2005-420.html</a>  Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Auditing Code Denial of Service  <a href="#">CAN-2005-0136</a>	Low	RedHat Security Advisory, RHSA-2005:420-22, June 8, 2005  <b>RedHat Security            Advisory,            RHSA-2005            :420-24,            Updated            August 9, 2005</b>

<p>Multiple Vendors</p> <p>Linux kernel 2.6.10, 2.6</p> <p>-test9-CVS, 2.6-test1-test11, 2.6, 2.6.1-2.6.11; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4</p>	<p>Multiple vulnerabilities exist: a vulnerability exists in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability exists in the 'setsid()' function; and a vulnerability exists in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges.</p> <p>RedHat: <a href="https://rhn.redhat.com/errata/RHSA-2005-092.html">https://rhn.redhat.com/errata/RHSA-2005-092.html</a></p> <p>Ubuntu: <a href="http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/">http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/</a></p> <p>Conectiva: <a href="ftp://atualizacoes.conectiva.com.br/">ftp://atualizacoes.conectiva.com.br/</a></p> <p>SUSE: <a href="ftp://ftp.SUSE.com/pub/SUSE">ftp://ftp.SUSE.com/pub/SUSE</a></p> <p>Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</a></p> <p>Conectiva: <a href="ftp://atualizacoes.conectiva.com.br/10/">ftp://atualizacoes.conectiva.com.br/10/</a></p> <p>Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p>RedHat: <a href="http://rhn.redhat.com/errata/RHSA-2005-366.html">http://rhn.redhat.com/errata/RHSA-2005-366.html</a></p> <p>RedHat: <a href="http://rhn.redhat.com/errata/RHSA-2005-283.html">http://rhn.redhat.com/errata/RHSA-2005-283.html</a></p> <p><a href="http://rhn.redhat.com/errata/RHSA-2005-284.html">http://rhn.redhat.com/errata/RHSA-2005-284.html</a></p> <p>RedHat: <a href="http://rhn.redhat.com/errata/RHSA-2005-472.html">http://rhn.redhat.com/errata/RHSA-2005-472.html</a></p> <p>Avaya: <a href="http://support.avaya.com/elmodocs2/security/ASA-2005-120">http://support.avaya.com/elmodocs2/security/ASA-2005-120</a> <a href="#">RHSA-2005-283</a> <a href="#">RHSA-2005-284</a> <a href="#">RHSA-2005-293</a> <a href="#">RHSA-2005-472.pdf</a></p> <p>FedoraLegacy: <a href="http://download.fedoralegacy.org/redhat/">http://download.fedoralegacy.org/redhat/</a></p> <p><b>RedHat:</b> <a href="http://rhn.redhat.com/errata/RHSA-2005-420.html">http://rhn.redhat.com/errata/RHSA-2005-420.html</a></p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	<p>Linux Kernel Multiple Vulnerabilities</p> <p><a href="#">CAN-2005-0176</a> <a href="#">CAN-2005-0177</a> <a href="#">CAN-2005-0178</a> <a href="#">CAN-2005-0204</a></p>	<p>Medium</p>	<p>Ubuntu Security Notice, USN-82-1, February 15, 2005</p> <p>RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005</p> <p>Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005</p> <p>Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005</p> <p>Fedora Update Notification FEDORA-2005-313, April 11, 2005</p> <p>RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005</p> <p>RedHat Security Advisories, RHSA-2005:283-15 &amp; RHSA-2005:284-11, April 28, 2005</p> <p>RedHat Security Advisory, RHSA-2005:472-05, May 25, 2005</p> <p>Avaya Security Advisory, ASA-2005-120, June 3, 2005</p> <p>FedoraLegacy: FLSA:152532, June 4, 2005</p> <p><b>RedHat Security Advisory, RHSA-2005:420-24, Updated August 9, 2005</b></p>
<p>Multiple Vendors</p> <p>SuSE Linux Professional 9.3, x86_64, 9.2, x86_64, Linux Personal 9.3, x86_64; Linux kernel 2.6-2.6.12</p>	<p>A buffer overflow vulnerability has been reported in the XFRM network architecture code due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary code.</p> <p>Patches available at: <a href="http://www.kernel.org/">http://www.kernel.org/</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Linux Kernel XFRM Array Index Buffer Overflow</p> <p><a href="#">CAN-2005-2456</a></p>	<p>High</p>	<p>Security Focus, 14477, August 5, 2005</p>

Multiple Vendors  Linux kernel 2.6-2.6.12 .1	<p>Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to an error when handling keyrings; and a Denial of Service vulnerability was reported in the 'KEYCTL_JOIN_SESSION_KEYRING' operation due to an error when attempting to join a key management session.</p> <p>Patches available at:  <a href="http://kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.13-rc6-git.1.bz2">http://kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.13-rc6-git.1.bz2</a></p> <p>There is no exploit code required.</p>	Linux Kernel Management Denials of Service  <a href="#">CAN-2005-2098</a> <a href="#">CAN-2005-2099</a>	Low	Secunia Advisory: SA16355, August 9, 2005
Multiple Vendors  zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	<p>A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input.</p> <p>Zlib:  <a href="http://www.zlib.net/zlib-1.2.3.tar.gz">http://www.zlib.net/zlib-1.2.3.tar.gz</a></p> <p>Debian:  <a href="http://security.debian.org/pool/updates/main/z/zlib/">http://security.debian.org/pool/updates/main/z/zlib/</a></p> <p>Ubuntu:  <a href="http://security.ubuntu.com/ubuntu/pool/main/z/zlib/">http://security.ubuntu.com/ubuntu/pool/main/z/zlib/</a></p> <p>OpenBSD:  <a href="http://www.openbsd.org/errata.html#libz2">http://www.openbsd.org/errata.html#libz2</a></p> <p>Mandriva:  <a href="http://www.mandriva.com/security/advisories?name=MDKSA-2005:124">http://www.mandriva.com/security/advisories?name=MDKSA-2005:124</a></p> <p>Fedora:  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p>Slackware:  <a href="http://slackware.com/security/viewer.php?l=slackware-security&amp;y=2005&amp;m=slackware-security.323596">http://slackware.com/security/viewer.php?l=slackware-security&amp;y=2005&amp;m=slackware-security.323596</a></p> <p>FreeBSD:  <a href="ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:18.zlib.asc">ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:18.zlib.asc</a></p> <p>SUSE:  <a href="http://lists.suse.com/archive/suse-security-announce/2005-Jul/0007.html">http://lists.suse.com/archive/suse-security-announce/2005-Jul/0007.html</a></p> <p>Gentoo:  <a href="http://security.gentoo.org/glsa/glsa-200507-28.xml">http://security.gentoo.org/glsa/glsa-200507-28.xml</a>   <a href="http://security.gentoo.org/glsa/glsa-200508-01.xml">http://security.gentoo.org/glsa/glsa-200508-01.xml</a></p> <p><b>Trustix:</b>  <a href="ftp://ftp.trustix.org/pub/trustix/updates/">ftp://ftp.trustix.org/pub/trustix/updates/</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service  <a href="#">CAN-2005-1849</a>	Low	<p>Security Focus, 14340, July 21, 2005</p> <p>Debian Security Advisory DSA 763-1, July 21, 2005</p> <p>Ubuntu Security Notice, USN-151-1, July 21, 2005</p> <p>OpenBSD, Release Errata 3.7, July 21, 2005</p> <p>Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005</p> <p>Secunia, Advisory: SA16195, July 25, 2005</p> <p>Slackware Security Advisory, SSA:2005-203-03, July 22, 2005</p> <p>FreeBSD Security Advisory, SA-05:18, July 27, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:043, July 28, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200507-28, July 30, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200508-01, August 1, 2005</p> <p><b>Trustix Secure Linux Security Advisory, TLSA-2005-0040, August 5, 2005</b></p>
netpbm 10.0	<p>A vulnerability has been reported in netpbm ('-dSAFER') that could let malicious users execute arbitrary postscript code.</p> <p>Trustix:  <a href="ftp://ftp.trustix.org/pub/trustix/updates/">ftp://ftp.trustix.org/pub/trustix/updates/</a></p> <p><b>Gentoo:</b>  <a href="http://security.gentoo.org/glsa/glsa-200508-04.xml">http://security.gentoo.org/glsa/glsa-200508-04.xml</a></p> <p>There is no exploit code required.</p>	netpbm Arbitrary Code Execution  <a href="#">CAN-2005-2471</a>	High	<p>Secunia Advisory: SA16184, July 25, 2005</p> <p>Trustix Secure Linux Security Advisory, #2005-0038, July 29, 2005</p> <p><b>Gentoo Linux Security Advisory, GLSA 200508-04, August 5, 2005</b></p>

ProFTPD	<p>Multiple format string vulnerabilities have been reported in ProFTPD that could let remote malicious users cause a denial of service or disclose information.</p> <p>Upgrade to version 1.3.0rc2:  <a href="http://www.proftpd.org/">http://www.proftpd.org/</a></p> <p>Gentoo:  <a href="http://www.gentoo.org/security/en/glsa/glsa-200508-02.xml">http://www.gentoo.org/security/en/glsa/glsa-200508-02.xml</a></p> <p><b>Trustix:</b>  <a href="ftp://ftp.trustix.org/pub/trustix/updates/">ftp://ftp.trustix.org/pub/trustix/updates/</a></p> <p><b>TurboLinux:</b>  <a href="ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/">ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	ProFTPD Denial of Service or Information Disclosure  <a href="#">CAN-2005-2390</a>	Medium	<p>Secunia, Advisory: SA16181, July 26, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200508-02, August 1, 2005</p> <p><b>Trustix Secure Linux Security Advisory, TLSA-2005-0040, August 5, 2005</b></p> <p><b>Turbolinux Security Advisory, TLSA-2005-82, August 9, 2005</b></p>
<p>Sun Microsystems, Inc.</p> <p>Solaris 10.0, 10.0_x86, 9.0, 9.0_x86 Update 2, 9.0_x86, 8.0, 8.0_x86, 7.0, 7.0_x86</p>	<p>A vulnerability has been reported in the 'printd' daemon due to an unspecified error, which could let a local/remote malicious user delete arbitrary files.</p> <p>Patches available at:  <a href="http://sunsolve.sun.com/search/document.do?assetkey=1-26-101842-1">http://sunsolve.sun.com/search/document.do?assetkey=1-26-101842-1</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Sun Solaris Printd Arbitrary File Deletion	Medium	Sun(sm) Alert Notification, 101842, August 8, 2005
<p>SysCP</p> <p>SysCP 1.2.1-1.2.10</p>	<p>Several vulnerabilities have been reported: a vulnerability was reported due to insufficient verification of input in an unspecified parameter before including a language file, which could let a remote malicious user include arbitrary files from external resources; and a vulnerability was reported in the internal template engine due to insufficient sanitization of input, which could let a remote malicious user execute arbitrary PHP code.</p> <p>Upgrades available at:  <a href="http://www.syscp.de/files/downloads/syscp-1.2.11.tar.gz">http://www.syscp.de/files/downloads/syscp-1.2.11.tar.gz</a></p> <p>There is no exploit code required; however a Proof of Concept exploit has been published.</p>	SysCP Multiple Script Execution	High	Secunia Advisory: SA16347, August 8, 2005
<p>Wine</p> <p>Windows API Emulator 20050725</p>	<p>A vulnerability has been reported in 'winelauncher.in' due to the insecure creation of a temporary file in '/tmp,' which could let a malicious user create/overwrite arbitrary files.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	Wine Wine Launcher.IN Local Insecure File Creation	Medium	Security Focus 14495, August 8, 2005
<p>Wojtek Kaniewski</p> <p>ekg 2005-06-05 22:03</p>	<p>A vulnerability has been reported in 'contrib/scripts/linki.py' due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges.</p> <p>Debian:  <a href="http://security.debian.org/pool/updates/main/e/ekg/">http://security.debian.org/pool/updates/main/e/ekg/</a></p> <p><b>Ubuntu:</b>  <a href="http://security.ubuntu.com/ubuntu/pool/main/e/ekg/">http://security.ubuntu.com/ubuntu/pool/main/e/ekg/</a></p> <p>There is no exploit code required.</p>	<p>Wojtek Kaniewski EKG Insecure Temporary File Creation</p> <p><a href="#">CAN-2005-1916</a></p>	Medium	<p>Secunia Advisory: SA15889, July 5, 2005</p> <p>Debian Security Advisory, DSA 760-1, July 18, 2005</p> <p><b>Ubuntu Security Notice, USN-162-1, August 08, 2005</b></p>
<p>Wojtek Kaniewski</p> <p>Eksperty-mentalny Klient Gadu-Gadu (ekg) 2005-04-11</p>	<p>Several vulnerabilities have been reported: a vulnerability was reported in 'contrib/ekgnv.sh,' 'contrib/getekg.sh,' and 'contrib/ekgh' due to the insecure creation of a temporary file, which could let a remote malicious user create/overwrite arbitrary files; and an SQL injection vulnerability was reported in 'contrib/scripts/ekgbot-pre1.py' due to an error, which could let a remote malicious user inject arbitrary shell commands.</p> <p>Debian:  <a href="http://security.debian.org/pool/updates/main/e/ekg/">http://security.debian.org/pool/updates/main/e/ekg/</a></p> <p><b>Ubuntu:</b>  <a href="http://security.ubuntu.com/ubuntu/pool/main/e/ekg/">http://security.ubuntu.com/ubuntu/pool/main/e/ekg/</a></p> <p>There is no exploit code required.</p>	<p>Wojtek Kaniewski EKG Insecure Temporary File Creation &amp; SQL Injection</p> <p><a href="#">CAN-2005-1850</a>  <a href="#">CAN-2005-1851</a></p>	High	<p>Debian Security Advisory, DSA 760-1, July 18, 2005</p> <p><b>Ubuntu Security Notice, USN-162-1, August 08, 2005</b></p>

Yukihiro Matsumoto Ruby 1.8.2	<p>A vulnerability has been reported in the XMLRPC server due to a failure to set a valid default value that prevents security protection using handlers, which could let a remote malicious user execute arbitrary code.</p> <p>Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p>TurboLinux: <a href="ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/">ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/</a></p> <p>Debian: <a href="http://security.debian.org/pool/updates/main/r/ruby1.8/">http://security.debian.org/pool/updates/main/r/ruby1.8/</a></p> <p>Gentoo: <a href="http://security.gentoo.org/glsa/glsa-200507-10.xml">http://security.gentoo.org/glsa/glsa-200507-10.xml</a></p> <p>Mandriva: <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a></p> <p><b>RedHat:</b> <a href="http://rhn.redhat.com/errata/RHSA-2005-543.html">http://rhn.redhat.com/errata/RHSA-2005-543.html</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Yukihiro Matsumoto Ruby XMLRPC Server Unspecified Command Execution  <a href="#">CAN-2005-1992</a>	High  Fedora Update Notifications, FEDORA-2005-474 & 475, June 21, 2005  Turbolinux Security Advisory, TLSA-2005-74, June 28, 2005  Debian Security Advisory, DSA 748-1, July 11, 2005  Gentoo Linux Security Advisory, GLSA 200507-10, July 11, 2005  Mandriva Linux Security Update Advisory, MDKSA-2005:118, July 13, 2005  <b>RedHat Security Advisory, RHSA-2005:543-08, August 5, 2005</b>
----------------------------------	--	--	--

[\[back to top\]](#)

Multiple Operating Systems - Windows / UNIX / Linux / Other				
Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apache	<p>A vulnerability has been reported in Apache which can be exploited by remote malicious user to smuggle http requests.</p> <p>Conectiva: <a href="http://distro.conectiva.com.br/atualizacoes/index.php?id=a&amp;anuncio=000982">http://distro.conectiva.com.br/atualizacoes/index.php?id=a&amp;anuncio=000982</a></p> <p>Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p><b>Mandriva:</b> <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a>  <a href="http://security.ubuntu.com/ubuntu/pool/main/a/apache2/">http://security.ubuntu.com/ubuntu/pool/main/a/apache2/</a></p> <p><b>TurboLinux:</b> <a href="ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/">ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/</a></p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	<p>Apache HTTP Request Smuggling Vulnerability</p> <p><a href="#">CAN-2005-1268</a> <a href="#">CAN-2005-2088</a></p>	Medium	<p>Secunia, Advisory: SA14530, July 26, 2005</p> <p>Conectiva, CLSA-2005:982, July 25, 2005</p> <p>Fedora Update Notification FEDORA-2005-638 &amp; 639, August 2, 2005</p> <p><b>Mandriva Linux Security Update Advisory, MDKSA-2005:129, August 3, 2005</b></p> <p><b>Ubuntu Security Notice, USN-160-1, August 04, 2005</b></p> <p><b>Turbolinux Security Advisory, TLSA-2005-81, August 9, 2005</b></p>
Chipmunk Scripts Chipmunk Forum 1.3	<p>A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'fontcolor' parameter, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proofs of Concept exploits have been published.</p>	<p>Chipmunk Forum 'fontcolor' Cross-Site Scripting</p>	Medium	<p>Security Tracker Alert ID: 1014630, August 8, 2005</p>
Cisco Cisco IOS 12.4 & prior 12.x versions	<p>An IPv6 packet handling vulnerability has been reported in Cisco IOS that could let local malicious users cause a remote Denial of Service or potentially execute arbitrary code.</p> <p>Vendor fix available: <a href="http://www.cisco.com/warp">http://www.cisco.com/warp</a></p>	<p>Cisco IOS Remote Denial of Service or Arbitrary Code Execution</p> <p><a href="#">CAN-2005-2451</a></p>	High	<p>Cisco Security Advisory, Document ID: 65783 Revision 1.5, August 1, 2005</p> <p><a href="#">US-CERT VU#930892</a></p>

</public/707/cisco-sa-20050729-ipv6.shtml#software>

**Revision 1.6: Added a note to the Affected Products section. Software Versions and Fixes table updated for 12.2EZ.**

**Revision 1.7: Software Versions and Fixes table updated for Cisco IOS XR.**

A working Proof of Concept exploit has been developed; however, it is currently not publicly available.

**Cisco Security Advisory, Document ID: 65783 Revision 1.6 & 1.7, August 3 & 5, 2005**

Comdev Software eCommerce 3.0	<p>A Directory Traversal vulnerability has been reported in 'WCE.Download.php,' which could let a remote malicious user obtain sensitive information.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept has been published.</p>	Comdev eCommerce 'WCE.Download. PHP' Directory Traversal  <a href="#">CAN-2005-2543</a>	Medium	Security Focus, 14479, August 5, 2005
Comdev Software eCommerce 3.0	<p>A vulnerability has been reported in the 'path[docroot]' parameter due to insufficient verification before including files, which could let a remote malicious user execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept has been published.</p>	Comdev ECommerce Config.PHP Remote File Include  <a href="#">CAN-2005-2544</a>	High	Secunia Advisory: SA16346, August 8, 2005
Denora IRC Stats Denora IRC Stats 1.0	<p>A buffer overflow vulnerability has been reported in the 'rdb_query()' function due to a boundary error, which could let a remote malicious user execute arbitrary code.</p> <p>Upgrade available at: <a href="http://denora.nomadirc.net/download.php">http://denora.nomadirc.net/download.php</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Denora IRC Stats Remote Buffer Overflow  <a href="#">CAN-2005-2484</a>	High	Secunia Advisory: SA16281, August 4, 2005
e107.org  e107 website system 0.617, 0.616, 0.603, 0.6 10 - 0.6 15a	<p>Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because users can upload HTML and TXT attachments that contain JavaScript, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published for the Cross-Site Scripting vulnerability.</p>	E107 Website System Cross-Site Scripting & HTML Injection	Medium	Security Focus, 14495 & 14508, August 8, 2005
EMC  Navisphere Manager 6.4-6.6	<p>Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported due to insufficient validation of HTTP requests, which could let a remote malicious user obtain sensitive information; and an information disclosure vulnerability was reported because it is possible to list the contents of a directory.</p> <p>The vendor has addressed this issue in the latest version of the affected application.</p> <p>There is no exploit code required; however, Proofs of Concept exploits have been published.</p>	EMC Navisphere Manager IEMC Navisphere Manager Directory Traversal & Information Disclosure  <a href="#">CAN-2005-2357</a> <a href="#">CAN-2005-2358</a>	Medium	iDEFENSE Security Advisory, August 5, 2005
Ethereal  Ethereal V0.10.11	<p>Multiple dissector and zlib vulnerabilities have been reported in Ethereal that could let remote malicious users cause a denial of service or execute arbitrary code.</p> <p>Upgrade to version 0.10.12: <a href="http://www.ethereal.com/download.html">http://www.ethereal.com/download.html</a></p> <p>Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a></p> <p><b>Mandriva:</b> <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a></p> <p>Currently we are not aware of any exploits for these vulnerabilities.</p>	Ethereal Denial of Service or Arbitrary Code Execution  <a href="#">CAN-2005-2361</a> <a href="#">CAN-2005-2362</a> <a href="#">CAN-2005-2363</a> <a href="#">CAN-2005-2364</a> <a href="#">CAN-2005-2365</a> <a href="#">CAN-2005-2366</a> <a href="#">CAN-2005-2367</a>	High	Secunia, Advisory: SA16225, July 27, 2005  <b>Mandriva Linux Security Update Advisory, MDKSA-2005:131, August 4, 2005</b>

FFTW FFTW 3.0.1	<p>A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user create/overwrite arbitrary files.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	FFTW Insecure Temporary File Creation	Medium	Security Focus, 14501, August 8, 2005
FlatNuke FlatNuke 2.5.5	<p>Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'structure.php' due to insufficient sanitization of the 'bodycolor,' 'backimage,' 'theme,' and 'logo' parameters, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported due to insufficient sanitization of posted news articles before displaying to site administrators, which could let a remote malicious user execute arbitrary code; a vulnerability was ported due to insufficient sanitization of the 'firma' parameter when saving the user's signature to the user file, which could let a remote malicious user inject and execute arbitrary PHP commands; and a vulnerability was reported because it is possible to obtain path information.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proofs of Concept exploits have been published.</p>	<p>FlatNuke Multiple Vulnerabilities</p> <p><a href="#">CAN-2005-2537</a>  <a href="#">CAN-2005-2538</a>  <a href="#">CAN-2005-2539</a>  <a href="#">CAN-2005-2540</a></p>	High	Secunia Advisory: SA16330, August 5, 2005
FunkBoard FunkBoard 0.66 CF	<p>Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proofs of Concept exploits have been published.</p>	FunkBoard Multiple Cross-Site Scripting	Medium	Security Focus, 13507, August 8, 2005
Fusebox Fusebox 4.1.0	<p>A Cross-Site Scripting vulnerability has been reported in the 'index.cfm' due to insufficient sanitization of the 'fuseaction' parameter, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been reported.</p>	<p>Fusebox 'Index.CFM' Cross-Site Scripting</p> <p><a href="#">CAN-2005-2480</a></p>	Medium	Security Focus, 14460, August 3, 2005
Gravity Board X Development GBX 1.1	<p>Multiple vulnerabilities have been reported: an SQL injection vulnerability was reported in 'index.php' due to insufficient sanitization of the 'email' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a Cross-Site Scripting vulnerability was reported in 'deletethread.php' due to insufficient sanitization of the 'board_id' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the 'editcss.php' script due to insufficient access restrictions, which could let a remote malicious user execute arbitrary PHP scripts.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proofs of Concept exploits and a script for the Cross-Site Scripting vulnerability have been published.</p>	Gravity Board X Input Validation & Access Restrictions	High	Security Tracker Alert ID: 1014631, August 8, 2005
Inkscape Inkscape 0.41	<p>A vulnerability has been reported in 'ps2epsi.sh' due to the insecure creation of a temporary file, which could let a malicious user create/overwrite arbitrary files.</p> <p>Upgrade available at:  <a href="http://citkit.dl.sourceforge.net/sourceforge/inkscape/inkscape-0.42.ta.r.gz">http://citkit.dl.sourceforge.net/sourceforge/inkscape/inkscape-0.42.ta.r.gz</a></p> <p>There is no exploit code required.</p>	Inkscape 'ps2epsi.sh' Insecure Temporary File	Medium	Security Focus 14522, August 9, 2005
Invision Power Services Invision Board 1.0.3	<p>a Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>Invision Power Board Cross-Site Scripting</p> <p><a href="#">CAN-2005-2542</a></p>	Medium	Security Focus, 14492, August 8, 2005
Jax Scripts Jax Petitionbook 3.31, Newsletter 2.14, Jax LinkLists 1.0 , Guestbook 3.31, Jax DWT	<p>Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p>	Jax PHP Scripts Multiple Cross-Site Scripting	Medium	Security Focus 14481, August 5, 2005

Editor 1.0, Jax Calendar 1.34	There is no exploit code required; however, a Proof of Concept has been published.			
Jax Scripts Jax Petitionbook 3.31, Newsletter 2.14, Jax LinkLists 1.0 , Guestbook 3.31, Jax DWT Editor 1.0, Jax Calendar 1.34	Multiple vulnerabilities have been reported due to insufficient access validation, which could let a remote malicious user obtain sensitive information.  No workaround or patch available at time of publishing.  There is no exploit code required; however, a Proof of Concept has been published.	Jax PHP Scripts Multiple Remote Information Disclosure	Medium	Security Focus 14482, August 5, 2005
Karrigell Karrigell 2.1-2.1.5, 2.0-2.0.5, 1.x	A vulnerability has been reported in a karrigell services (.ks) script due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary python code.  Upgrades available at: <a href="http://prdownloads.sourceforge.net/karrigell/Karrigell-2.1.8.tgz?download">http://prdownloads.sourceforge.net/karrigell/Karrigell-2.1.8.tgz?download</a>  There is no exploit code required; however, Proofs of Concept exploits have been published.	Karrigell Arbitrary Python Code Execution  <a href="#">CAN-2005-2483</a>	High	Secunia Advisory: SA16319, August 3, 2005
KDE KDE 3.4, 3.3-3.3.2, 3.2-3.2.3	A vulnerability has been reported in KDE Kate and KWrite because backup files are created with default permissions even if the original file had more restrictive permissions set, which could let a local/remote malicious user obtain sensitive information.  Patches available at: <a href="ftp://ftp.kde.org/pub/kde/security_patches/">ftp://ftp.kde.org/pub/kde/security_patches/</a>  Fedora: <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/</a>  Mandriva: <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a>  RedHat: <a href="http://rhn.redhat.com/errata/RHSA-2005-612.html">http://rhn.redhat.com/errata/RHSA-2005-612.html</a>  <b>Conectiva:</b> <a href="ftp://atualizacoes.conectiva.com.br/">ftp://atualizacoes.conectiva.com.br/</a>  There is no exploit code required.	KDE Kate, KWrite Local Backup File Information Disclosure  <a href="#">CAN-2005-1920</a>	Medium	Security Tracker Alert ID: 1014512, July 18, 2005  Fedora Update Notification, FEDORA-2005-594, July 19, 2005  Mandriva Linux Security Update Advisory, MDKSA-2005:122, July 20, 2005  RedHat Security Advisory, RHSA-2005:612-07, July 27, 2005  <b>Conectiva Linux Announcement, CLSA-2005:988, August 4, 2005</b>
Lansoft Enterprises OpenBB 1.1 .0	Multiple SQL injection vulnerabilities have been reported in 'board.php,' read.php,' and member.php' due to insufficient sanitization of the 'FID,' 'TID,' and 'UID' parameters before used in a SQL query, which could let a malicious user execute arbitrary SQL code.  No workaround or patch available at time of publishing.  There is no exploit code required; however, Proofs of Concept exploits have been published.	OpenBB Multiple SQL Injection	Medium	Secunia Advisory: SA16369, August 9, 2005
Logicampus Logicampus 1.1 .0	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to the helpdesk before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code.  Upgrade available at: <a href="http://prdownloads.sourceforge.net/logicampus/logicampus-1.1.1.tar.gz?download">http://prdownloads.sourceforge.net/logicampus/logicampus-1.1.1.tar.gz?download</a>  There is no exploit code required.	LogiCampus Helpdesk Cross-Site Scripting  <a href="#">CAN-2005-2485</a>	Medium	Security Focus, 14472, August 4, 2005
McDATA Sphereon Fabric Switch 4500, 4300, Intrepid Director Switch 6140, 6064, McDATA E/OS	A remote Denial of Service vulnerability has been reported due to a failure to recover from network broadcast storms.  Update to E/OS 6.0.0 or later (E/OS 7.01.00 in patch 119550-01 also contains the fix).  Sun: <a href="http://sunsolve.sun.com/search/document.do?assetkey=1-21-119550-01-1">http://sunsolve.sun.com/search/document.do?assetkey=1-21-119550-01-1</a>  There is no exploit code required.	McDATA E/OS Remote Denial of Service  <a href="#">CAN-2005-2487</a>	Low	Sun(sm) Alert Notification, 101833, August 3, 2005  Secunia Advisory: SA16295, August 4, 2005

Metasploit Project Metasploit Framework 2.0-2.4, 1.0	<p>A vulnerability has been reported in the 'StateToOptions()' function because the '_Defanged' environment variable can be overwritten, which could let a remote malicious user bypass security restrictions.</p> <p>Contact the vendor for further information on obtaining fixes.</p> <p>There is no exploit code required.</p>	Metasploit Framework MSFWeb Defanged Mode Restriction Bypass <a href="#">CAN-2005-2482</a>	Medium	Secunia Advisory: SA16318, August 2, 2005
myFAQ myFAQ 1.0	<p>SQL injection vulnerabilities have been reported due to insufficient sanitization of the 'Theme,' 'SousTheme,' 'Question,' and 'Faq' parameters before using in SQL queries, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	MyFAQ Multiple SQL Injection	Medium	SVadvisory#13, August 6, 2005
MySQL AB MySQL 5.0 .0-0-5.0.4, 4.1 .0-0-4.1.5, 4.0.24, 4.0.21, 4.0.20 , 4.0.18, 4.0 .0-4.0.15	<p>A buffer overflow vulnerability has been reported due to insufficient bounds checking of data that is supplied as an argument in a user-defined function, which could let a remote malicious user execute arbitrary code.</p> <p>This issue is reportedly addressed in MySQL versions 4.0.25, 4.1.13, and 5.0.7-beta available at: <a href="http://dev.mysql.com/downloads/">http://dev.mysql.com/downloads/</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	MySQL User-Defined Function Buffer Overflow	High	Security Focus 14509 , August 8, 2005
PHP-Fusion PHP-Fusion 6.0.105, 6.0.106, 5.0 1 Service Pack, 5.0, 4.0 1, 4.00	<p>An SQL injection vulnerability was reported in 'Messages.php' script due to insufficient input validation before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	PHP-Fusion 'Messages.PHP' SQL Injection	Medium	Security Focus 14489, August 6, 2005
PHPLite Calendar Express 2.0	<p>Several vulnerabilities have been reported: an SQL injection vulnerability was reported in several scripts due to insufficient sanitization of the 'cid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in 'search.php' due to insufficient sanitization of the 'allwords' parameter, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proofs of Concept exploits have been published.</p>	Calendar Express SQL Injection & Cross-Site Scripting	Medium	Secunia Advisory: SA16353, August 9, 2005
PHPMailer PHPMailer 1.7-1.7.2	<p>A remote Denial of Service vulnerability has been reported in 'class.smtp.php' due to an error when processing overly long headers in the 'Data()' function.</p> <p><b>PHPMailer:</b> <a href="http://prdownloads.sourceforge.net/phpmailer/phpmailer-1.73.tar.gz?download">http://prdownloads.sourceforge.net/phpmailer/phpmailer-1.73.tar.gz?download</a></p> <p><b>Xoops:</b> <a href="http://www.xoops.org/modules/core/visit.php?cid=7&amp;lid=85">http://www.xoops.org/modules/core/visit.php?cid=7&amp;lid=85</a></p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	PHPMailer 'Data()' Function Remote Denial of Service <a href="#">CAN-2005-1807</a>	Low	Security Tracker Alert, 1014069, May 28, 2005  <b>Security Focus, 13805, August 9, 2005</b>
PHPOpenChat PHPOpenChat 3.0.2	<p>Multiple Cross-Site Scripting vulnerabilities. have been reported due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	PHPOpenChat Multiple Cross-Site Scripting <a href="#">CAN-2005-2545</a>	Medium	HSC Security Group Advisory, August 5, 2005
PHPSiteStats PHPSiteStats 1.0	<p>A vulnerability has been reported in the login script due to an unspecified error, which could let a remote malicious user bypass authentication routines.</p> <p>Update available at: <a href="http://prdownloads.sourceforge.net/phpsitestats/phpsitestats1.1.zip?download">http://prdownloads.sourceforge.net/phpsitestats/phpsitestats1.1.zip?download</a></p> <p>There is no exploit code required.</p>	PHPSiteStats Authentication Bypass	Medium	Secunia Advisory: SA16361, August 8, 2005

PortailPHP PortailPHP 2.4	<p>An SQL injection vulnerability has been reported in 'Index.php' due to insufficient sanitization before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>PortailPHP 'Index.PHP' SQL Injection</p> <p><a href="#">CAN-2005-2486</a></p>	Medium	Security Focus, 14474, August 4, 2005
SilverNews SilverNews 2.0.3	<p>An SQL injection vulnerability has been reported in 'Admin.php' due to insufficient sanitization of the username before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code or bypass authentication to obtain access to the administrative section.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>SilverNews 'Admin.PHP' SQL Injection</p> <p><a href="#">CAN-2005-2478</a></p>	Medium	Security Focus, 14466, August 3, 2005
SquirrelMail SquirrelMail 1.4.0 through 1.4.4	<p>Multiple vulnerabilities have been reported that could let remote malicious users conduct Cross-Site Scripting attacks.</p> <p>Upgrade to 1.4.4 and apply patch: <a href="http://prdownloads.sourceforge.net/squirrelmail/sqm-144-xss.patch">http://prdownloads.sourceforge.net/squirrelmail/sqm-144-xss.patch</a></p> <p>Gentoo: <a href="http://security.gentoo.org/glsa/glsa-200506-19.xml">http://security.gentoo.org/glsa/glsa-200506-19.xml</a></p> <p>Mandriva: <a href="http://www.mandriva.com/security/advisories">http://www.mandriva.com/security/advisories</a></p> <p>Debian: <a href="http://security.debian.org/pool/updates/main/s/squirrelmail/">http://security.debian.org/pool/updates/main/s/squirrelmail/</a></p> <p><b>RedHat:</b> <a href="http://rhn.redhat.com/errata/RHSA-2005-595.html">http://rhn.redhat.com/errata/RHSA-2005-595.html</a></p> <p>There is no exploit code required.</p>	<p>SquirrelMail Cross-Site Scripting Vulnerabilities</p> <p><a href="#">CAN-2005-1769</a></p>	Medium	<p>SquirrelMail Advisory, June 15, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200506-19, June 21, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:108, July 1, 2005</p> <p>Debian Security Advisory , DSA 756-1, July 13, 2005</p> <p><b>RedHat Security Advisory, RHSA-2005:595-12, August 3, 2005</b></p>
SquirrelMail SquirrelMail 1.4.0-1.4.5-RC1.	<p>A vulnerability has been reported in 'options_identities.php' because parameters are insecurely extracted, which could let a remote malicious user execute arbitrary HTML and script code, or obtain/manipulate sensitive information.</p> <p>Upgrades available at: <a href="http://www.squirrelmail.org/download.php">http://www.squirrelmail.org/download.php</a></p> <p>Debian: <a href="http://security.debian.org/pool/updates/main/s/squirrelmail/">http://security.debian.org/pool/updates/main/s/squirrelmail/</a></p> <p><b>RedHat:</b> <a href="http://rhn.redhat.com/errata/RHSA-2005-595.html">http://rhn.redhat.com/errata/RHSA-2005-595.html</a></p> <p>There is no exploit code required.</p>	<p>SquirrelMail Variable Handling</p> <p><a href="#">CAN-2005-2095</a></p>	High	<p>GulfTech Security Research Advisory, July 13, 2005</p> <p>Debian Security Advisory, DSA 756-1, July 13, 2005</p> <p><b>RedHat Security Advisory, RHSA-2005:595-12, August 3, 2005</b></p>
tDiary tDiary 2.1.1, 2.0.1	<p>A vulnerability has been reported due to a failure to perform validity checks on user's requests, which could let a remote malicious user edit/delete entries or configurations.</p> <p>Upgrades available at: <a href="http://prdownloads.sourceforge.net/tdiary/tdiary-full-2.0.2.tar.gz?download">http://prdownloads.sourceforge.net/tdiary/tdiary-full-2.0.2.tar.gz?download</a></p> <p>There is no exploit code required.</p>	<p>TDiary Cross-Site Request Forgery</p> <p><a href="#">CAN-2005-2411</a></p>	Medium	Security Focus, 14500, August 8, 2005

Web Content Management	A Cross-Site Scripting vulnerability has been reported a vulnerability in 'Includes/validsession.php' due to insufficient due to insufficient satiation of the 'strRootpath' parameter and in 'Admin/News/List.php' due to insufficient sanitization of the 'strTable' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the 'Admin/Users/AddModifyInput.php' script due to insufficient authentication, which could let a remote malicious user obtain administrative privileges.	Web Content Management Cross-Site Scripting & Authentication Bypass  <a href="#">CAN-2005-2488</a> <a href="#">CAN-2005-2489</a>	Medium	Security Tracker Alert ID: 1014616, August 3, 2005
Web Content Management	No workaround or patch available at time of publishing.			
	There is no exploit code required; however, Proofs of Concept exploits and script have been published.			
XMB Forum	An SQL injection vulnerability has been reported in 'U2U.Inc.PHP' due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.	XMB Forum U2U.Inc.PHP SQL Injection	Medium	Security Focus 14523, August 9, 2005
XMB Forum .9.1	No workaround or patch available at time of publishing.			
	There is no exploit code required.			

[\[back to top\]](#)

## Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- Bluetooth: Those Spying Eyes:** Security concerns regarding the use of Bluetooth technology is on the rise. According to Ollie Whitehouse, architect of Symantec's research division, infiltration is possible anywhere large groups of people are using Bluetooth for extended periods, e.g., in an airport. Whitehouse and his colleagues have coined the term "war nibbling" to describe the act of taking a lot of small bits of data. Source: <http://www.varbusiness.com/showArticle.jhtml;jsessionid=SAPFFS2NWZRBOQS.NDBCSKHSCJUMEKJVN?articleID=166403057>.
- Wireless Networking Moves Into the Mainstream:** Infonetics Research, a networking market analyst and consulting firm based in the United States and Europe, recently published a study to determine product requirements and implementation plans of organizations that have implemented WLANs or will do so in the next year. Another goal of the study was to understand key deployment drivers. Source: <http://www.varbusiness.com/showArticle.jhtml;jsessionid=SAPFFS2NWZRBOQSNDBCSKH.SCJUMEKJVN?articleID=166403050>.
- Groups team up for Wi-Fi spec:** Three competing groups have agreed to work together on the proposed 802.11n wireless protocol. This is a move that could speed up ratification of the standard. Source: <http://www.itweek.co.uk/itweek/news/2140913/groups-team-wi-spec>.

### Wireless Vulnerabilities

- Nothing significant to report.

[\[back to top\]](#)

## Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

*Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
August 10, 2005	aircrack-2.21.tgz	N/A	An 802.11 WEP cracking program that can recover a 40-bit or 104-bit WEP key once enough encrypted packets have been gathered.
August 10, 2005	funkboard066.txt	No	Exploit details for the FunkBoard Multiple Cross-Site Scripting vulnerability.
August 10, 2005	openSQL.txt	No	Sample exploit for the OpenBB Multiple SQL Injection vulnerability.
August 10, 2005	scapy-1.0.0.tar.gz	N/A	A powerful interactive packet manipulation tool, packet generator, network scanner, network discovery tool, and packet sniffer.
August 8, 2005	GBX-CSS-exp.zip	No	Exploit script for the Gravity Board Cross-Site Scripting vulnerability.
August 6, 2005	citiBypass.txt	N/A	Write up that discusses a methodology to bypass Citibank Virtual Keyboard Protection, a mechanism to help protect against keyloggers and spyware.
August 6, 2005	JaxXSS.txt	No	Exploitation details for the Jax PHP Scripts Multiple Cross-Site Scripting vulnerabilities.
August 6, 2005	nbSMTP_fsexp.c	Yes	Exploit for the no-brainer SMTP Client 'log_msg' Format String vulnerability.
August 5, 2005	aircrack-2.2.tgz	N/A	Aircrack is an 802.11 WEP cracking program that can recover a 40-bit or 104-bit WEP key once enough encrypted packets have been gathered.
August 5, 2005	Easyxp41.txt	No	Exploit for the Easy PX41 CMS Cross-Site Scripting or Information Disclosure vulnerability.
August 5, 2005	edituserxp.sh	Yes	Proof of Concept exploit for the Lantronix Secure Console Server 'edituser' Buffer Overflow vulnerability.
August 5, 2005	eventum.pl.txt	Yes	Proof of Concept exploit for the MySQL Eventum SQL Injection vulnerability.

August 5, 2005	FlatNuke-codexec.zip flatnuke.html	No	Exploits for the FlatNuke User Data Arbitrary PHP Code Execution , Cross-Site Scripting, and Path Disclosure vulnerabilities.
August 5, 2005	phrack63.tar.gz	N/A	Phrack Magazine Issue 63 includes: Phrack Prophile on Tiago, OSX heap exploitation techniques, Hacking Windows CE, Games with kernel Memory...FreeBSD Style, Raising The Bar For Windows Rootkit Detection, Embedded ELF Debugging, Hacking Grub for Fun and Profit, Advanced antiforensics : SELF, Process Dump and Binary Reconstruction, Next-Gen. Runtime Binary Encryption, Shifting the Stack Pointer, NT Shellcode Prevention Demystified, PowerPC Cracking on OSX with GDB, Hacking with Embedded Systems, Process Hiding and The Linux Scheduler, Breaking Through a Firewall, Phrack World News.
August 5, 2005	pluggedBlog.txt	No	Detailed exploitation technique for the Plugged-Blog Multiple Vulnerabilities.
August 5, 2005	qlite.html	No	Proof of Concept exploit for the qliteNews arbitrary database manipulation and Cross-Site Scripting vulnerabilities.
August 5, 2005	webc.html	No	Proof of Concept exploit fir the Web Content Management Cross-Site Scripting & Authentication Bypass vulnerability.
August 5, 2005	yersinia-0.5.5.tar.gz	N/A	Yersinia implements several attacks for the following protocols: Spanning Tree (STP), Cisco Discovery (CDP), Dynamic Host Configuration (DHCP), Hot Standby Router (HSRP), Dynamic Trunking (DTP), 802.1q and VLAN Trunking (VTP), helping a pen-tester with different tasks.
August 3, 2005	CABrightStorSQL.c	Yes	Exploit for the the Computer Associates BrightStor ARCserve Backup Remote Buffer Overflow vulnerability.
August 2, 2005	prorat_server_dos.c	No	Proof of Concept Denial of Service exploit for the ProRat Server Remote Buffer Overflow vulnerability.

[back to top](#)

## Trends

- Get Up, Stand Up, Pharming Is On The Rise:** Pharming is one of the latest online scams and a rapidly growing threat that has been showing up on the Internet. It's a new way for criminals to try to get into your computer so they can steal your personal data that works by redirecting your Internet browser.  
Source: <http://www.crime-research.org/news/09.08.2005/1416/> .
- Scanning Activity on Port 6070/tcp:** US-CERT has seen reports indicating an increase in scanning activity of port 6070/tcp. This port is used by Computer Associates BrightStor ARCserve. Source: <http://www.us-cert.gov/current/>.
- ID theft ring hits 50 banks, security firm says:** A major identity theft ring discovered last weekly by Sunbelt Software, a security firm, has affected the customers of at least 50 banks. In a statement made by Sunbelt, the operation, which is being investigated by the FBI, is gathering personal data from "thousands of machines" using keystroke logging software. The data collected includes credit card details, Social Security numbers, usernames, passwords, instant messaging chat sessions and search term. Source: [http://news.zdnet.com/2100-1009\\_22-5823591.html](http://news.zdnet.com/2100-1009_22-5823591.html).
- Government computers top target for cyberattacks:** According to IBM's Global Business Security Index report, cyberattacks on computer systems escalated in the first half of 2005 and government agencies were targeted more than any other business sector, In the first half of 2005, there were more than 237 million security attacks worldwide, with 54 million directed at the U.S. government. The manufacturing sector received about 36 million attacks, followed by the financial services industry with 34 million and health care with 17 million. Source: <http://www.govexec.com/dailyfed/0805/080505p1.htm>.
- New Trend Found In IM Enterprise Threats:** A security firm, Akonix Systems, reported that nearly a quarter more new viruses threatening corporate computers through employee use of public instant-messaging networks were discovered in July. Including one that reflected a new trend of attacking multiple IM systems. A total of 42 new threats were tracked in July, a 24 percent increase over the previous month. Source: <http://www.techweb.com/wire/security/167101004>.
- U.S. Passes the Buck on Identity Theft:** A year ago President George W. Bush signed into law the Identity Theft Penalty Enhancement Act in response to the growing proliferation of Internet scams, such as phishing, pharming and other ploys aimed at stealing consumers' private information electronically. However, the evidence suggests that this new law has done nothing to reduce identity theft or fraud. The number of publicly known identity theft cases has increased dramatically over the past year. Since January of 2005, there have been over 63 data-security breaches exposing nearly 50 million identities. Source: [http://www.newsfactor.com/story.xhtml?story\\_id=37545](http://www.newsfactor.com/story.xhtml?story_id=37545).
- First potential virus risk for Windows Vista found:** Virus writers are targeting a new Microsoft tool that will be part of Windows and is set to ship as part of the next Exchange e-mail server release. According to F-Secure, a virus writer has published the first examples of malicious code that targets Microsoft's upcoming command-line shell, code-named Monad. If the technology is included in Windows Vista, these could be one of the first viruses to target the new operating system formerly known as Longhorn. Source: [http://news.zdnet.com/2100-1009\\_22-5819428.html?tag=zdfd.newsfeed](http://news.zdnet.com/2100-1009_22-5819428.html?tag=zdfd.newsfeed).

[back to top](#)

## Viruses/Trojans

### Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
------	-------------	--------------	-------	------	-------------

1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared files.
2	Mytob.C	Win32 Worm	Slight Increase	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
3	Zafi-D	Win32 Worm	Slight Decrease	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
4	Netsky-Q	Win32 Worm	Stable	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
5	Mytob-BE	Win32 Worm	Slight Decrease	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
6	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
7	Zafi-B	Win32 Worm	Increase	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
8	Netsky-D	Win32 Worm	Slight Increase	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
9	Netsky-Z	Win32 Worm	Decrease	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
10	Lovgate.w	Win32 Worm	Decrease	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.

Table updated August 6, 2005

[\[back to top\]](#)

**Last updated August 11, 2005**